Identification of Credit Card Fraud Utilizing Hybrid Deep Learning Models with Improved Precision and

Minimized False Positives

N Deshai1, Y Deva2, V Ravi Varma3, A Surya4, N Anil Kumar 5, M Chilakarao 6

1,2,3,4,5,6 Dept. of IT, SRKREC, (JNTUK), Bhimavaram A.P, India. [desaij4@gmail.com1,](mailto:desaij4@gmail.com1) [devayadhala04@gmail.com2,](mailto:devayadhala04@gmail.com2) [vatsavayiravi2003@gmail.com3,](mailto:vatsavayiravi2003@gmail.com3)

[suryaantarvedi@gmail.com4,](mailto:suryaantarvedi@gmail.com4) [anilkumar9866487017@gmail.com](mailto:anilkumar9866487017@gmail.com) 5, [chilakarao@gmail.com](mailto:chilakarao@gmail.com) 6.

Correspondence mail: desaij4@gmail.com

**Abstract.** Consumers and businesses face financial risks because of the increase in credit card fraud brought on by the boom in digital transactions. Traditional fraud detection technology can't keep up with evolving fraud strategies, which leads to high false positives and undetected fraud. This paper proposes a hybrid deep learning system that integrates Autoencoders, Conv1D, SMOTE, and LSTM to increase the accuracy of fraud detection. SMOTE addresses class imbalance, autoencoders extract complex transaction patterns, Conv1D detects local dependencies, and LSTM captures long-term temporal correlations. Class imbalance is addressed by SMOTE, complicated transaction patterns are extracted by autoencoders, local dependencies are detected by Conv1D, and long-term temporal correlations are captured by LSTM. When compared to traditional models, experimental results on the European Credit Card Dataset demonstrate improved precision, recall, and F1-score. The results highlight how crucial hybrid deep learning is to create adaptive fraud detection systems that can react to new fraud trends. To improve financial security, future work will concentrate on real-time deployment and enhancing model interpretability.

**Keywords:** Long Short-Term Memory (LSTM), Autoencoders, Hybrid Models, Credit Card Fraud, Fraud Detection, and Synthetic Minority Over- sampling Technique (SMOTE)

# Introduction

The rapid advancement of digital payment systems has revolutionized financial transactions, enabling seamless international purchases [1]. However, this growth has also led to a significant rise in credit card fraud, posing serious financial threats to both consumers and financial institutions【2】. Reports indicate that fraudulent transactions result in billions of dollars in losses annually, emphasizing the urgent need for more sophisticated fraud detection systems. Traditional rule-based and machine learning models struggle with high false positive rates, delayed fraud detection, and limited adaptability to evolving fraud strategies, ultimately compromising security and customer trust【3】.

A key challenge in fraud detection is the class imbalance within credit card transaction datasets, where fraudulent transactions constitute only a small fraction of the total records. This disparity biases models toward legitimate transactions, leading to misclassification of fraudulent activities. Additionally, static detection algorithms fail to address the constantly evolving fraud patterns, making them ineffective for real-time fraud prevention【4】.

To address these limitations, this paper proposes a hybrid deep learning framework that integrates Synthetic Minority Over-sampling Technique (SMOTE), Autoencoders, Conv1D, and Long Short-Term Memory (LSTM) to enhance fraud detection accuracy. SMOTE mitigates class imbalance, LSTM captures long-term temporal dependencies, autoencoders extract hidden transaction patterns, and Conv1D identifies spatial relationships within transactional data. This hybrid approach has demonstrated superior fraud detection performance with lower false positive rates, outperforming traditional models in precision, recall, and F1-score, as validated on the Credit Card Fraud Detection Dataset【5】.

The remainder of this paper is organized as follows:

Section II reviews existing credit card fraud detection techniques, analyzing their strengths and limitations.

Section III presents the proposed hybrid deep learning framework, detailing the model architecture, training methods, and data preparation.

Section IV describes the implementation process, including dataset preprocessing, model training, and evaluation setup.

Section V discusses the experimental results and comparative analysis, demonstrating the effectiveness of the proposed approach.

Section VI concludes the paper, highlighting key findings, limitations, and future research directions, with a focus on real-time deployment strategies and enhanced model interpretability for financial security applications.

.

# Literature Survey

Prabha and Priscilla et al. (2024) proposed a fraud detection model utilizing LSTM autoencoders with an attention mechanism for high-level feature extraction, followed by classification using XGBoost . Their approach, using an adaptive threshold (θ = 0.22), achieved 90.5% recall and 94.2% accuracy, significantly improving recall performance. When tested on the IEEE-CIS dataset, the model outperformed existing fraud detection techniques【6-7】.

Ileberi and Sun et al. demonstrated that their model surpasses individual fraud detection techniques, achieving an AUC-ROC of 0.972, sensitivity of 0.961, and specificity of 0.999 on the European Credit Card Dataset 【8-10】. Similarly, Sumaya S. Sulaiman et al. investigated deep learning models such as Autoencoder, CNN, and LSTM with hyperparameter tuning for fraud detection. Their study found that LSTM performed best, achieving 99.2% accuracy, a 93.3% detection rate, and a 96.3% AUC-ROC score. Their work also highlighted the class imbalance issue and successfully integrated SMOTE to enhance real-time fraud detection【11】.

Ibomoiye Domor Mienye et al. explored various deep learning models, including CNNs, RNNs, LSTMs, and GRUs, for fraud detection. Their research emphasized the robustness of deep learning over traditional machine learning techniques, particularly in handling class imbalance through data augmentation 【12-15】.

Fawaz Khaled Alarfaj et al. investigated the effectiveness of Graph Neural Networks (GNNs) and Autoencoders in fraud detection. Their study highlighted how these models enhance fraud prevention strategies and strengthen financial security 【16】.

Similarly, Iseal et al. examined the role of deep learning in reducing false positives and identifying complex fraud patterns, suggesting blockchain, federated learning, and enhanced data interpretability for future improvements【17】.

Dhandore et al. proposed a real-time fraud detection framework that enhances F1-score, recall, and accuracy while reducing false positives. Their work emphasized adaptive learning and real-time data processing to detect emerging fraud trends【18】.

Palivela et al. introduced a hybrid approach, utilizing CNNs for spatial feature extraction, LSTMs for temporal sequence analysis, and transformers for dependency modelling. Their model achieved AUC-ROC (0.972), specificity (0.999), and sensitivity (0.961) on the European Credit Card Dataset, demonstrating superior performance【19】.

San Miguel Carrasco et al. developed an Optimized Sequential Model for Fraud Detection, integrating hyperparameter tuning and ensemble learning techniques such as Random Forest, Gradient Boosting, Logistic Regression, and Voting Classifiers. Their model, using pre-processed transaction data and SMOTE for class balancing, significantly outperformed traditional fraud detection systems 【19】

# Methodology

A novel hybrid deep learning framework that combines several techniques, such as Autoencoders, Convolutional Neural Networks (Conv1D), Synthetic Minority Over-sampling Technique (SMOTE), and Long Short-Term Memory (LSTM) networks, is part of the suggested methodology for improving credit card fraud detection. The procedures listed below describe the thorough methodology utilized in the creation and deployment of the fraud detection system:

## Gathering and Preparing Data

* + 1. **Collection of Data:**

The Credit Card Dataset is used to train and evaluate models. It contains transaction records, with a small percentage of fraudulent transactions. Features include transaction amount, time, and other metadata, along with labels indicating whether each transaction is legitimate or fraudulent.

## Preprocessing:

Missing values are handled, and categorical variables are encoded if necessary. Normalization is applied to the features to scale the values to a similar range, ensuring consistent input for the deep learning models.

## Using the Synthetic Minority Over-sampling Technique (SMOTE) to Address Class Imbalance:

Class imbalance is addressed by SMOTE, which creates synthetic fraud samples by interpolating preexisting ones because fraudulent transactions are uncommon. By balancing the dataset, this lessens bias toward valid transactions and aids the model in efficiently learning fraud tendencies

## Feature Extraction using Autoencoders

Autoencoders extract complex transaction patterns by compressing and reconstructing data. The reconstruction error helps detect anomalies, while the encoder’s learned features enhance fraud detection in subsequent models.

## Sequential Data Processing with Conv1D

By using filters that identify time-based patterns and trends, Conv1D improves fraud detection across consecutive transactions by capturing local dependencies in transaction data.

## Temporal Relationships with LSTM Networks

Long-term dependencies in transaction sequences are captured by LSTM networks, which is essential for identifying changing fraud trends. They enhance anomaly detection by identifying sequential links in transactions. This aids in the detection of fraudulent activity that develops over time.

## Model Integration and Hybrid Framework

The hybrid model captures temporal and spatial fraud patterns by combining Autoencoder, Conv1D, and LSTM. Conv1D and LSTM processing are improved by autoencoder features, which also improve detection. Transactions are categorized as legal or fraudulent by a final thick layer.

## Training the Hybrid Model

The hybrid model is trained using binary cross-entropy and the Adam optimizer on an SMOTE-balanced dataset. Batch normalization and dropout prevent overfitting and guarantee better generalization.

## Metrics of Evaluation

A number of metrics are used to assess the model's performance, including:

* + 1. **Precision:** Calculates the percentage of all transactions that are detected as fraudulent that are accurately identified as such.

To calculate precision, use the formula --1.

|  |  |
| --- | --- |
|  | (1) |

**3.8.2 Recall:** Calculates the percentage of fraudulent transactions that were accurately identified out of all fraudulent transactions.

Formula-2 can be used to calculate recall.

|  |  |
| --- | --- |
|  | (2) |

* + 1. **F1-Score:** A balanced indicator of the model's performance that is calculated as the harmonic mean of precision and recall.

Equation 3's harmonic mean is the F1 Score.

(3)

**3.8.4** **Accuracy:** How well the model classifies transactions as either legitimate or fraudulent overall.

Formula -4 can be used to determine accuracy.

|  |  |
| --- | --- |
|  | (4) |
|  |  |
|  |  |

**3.8.5 ROC-AUC:** The receiver operates characteristic curve's area under the curve, which indicates how well the model can distinguish between classes.

The ROC-AUC score is computed by using formula 5:

|  |  |
| --- | --- |
|  | (5) |

Where as,

True Positive Rate (TPR) or Sensitivity:

TPR = 𝑇𝑃

𝑇𝑃+𝐹𝑁

False Positive Rate (FPR):

FPR = 𝐹𝑃

𝐹𝑃+𝑇𝑁

A diagram of a process

AI-generated content may be incorrect.

Figure 1: Fraud Detection Process

## Comparison with Baseline Models

Alternative deep learning models (e.g., standalone Autoencoders, Conv1D, LSTM) and traditional machine learning models (e.g., Random Forest, SVM) are compared to the proposed hybrid deep learning framework. Performance comparisons that focus on accuracy, precision, recall, F1-score, and false positive rate highlight the benefits of the hybrid strategy in controlling class imbalance and spotting new fraudulent activity.

## 3.10. Future Work and Deployment

To facilitate ongoing monitoring and the identification of fraudulent transactions, future research will concentrate on modifying the hybrid model for real- time implementation. Furthermore, to give financial institutions transparent decision-making and promote system confidence, efforts will be made to improve model interpretability through the use of strategies like SHAP (SHapley Additive exPlanations). In order to overcome the difficulties in detecting credit card fraud, this methodology emphasizes the integration of several deep learning techniques, especially when it comes to managing unbalanced data, identifying intricate patterns, and enhancing accuracy detection.

# Implementation

The hybrid model uses CNN and LSTM networks to capture temporal and spatial correlations in credit card transactions. The input layer receives the reprocessed transaction data. Conv1D layers identify local patterns, while LSTM layers document sequential dependencies. The Concatenation Layer combines CNN and LSTM feature extractions. A Fully Connected (Dense) Layer analyses the data for predictions, while a Dropout Layer prevents overfitting by randomly shutting off neurons. To ascertain if a transaction is fraudulent or not, the Output Layer employs a sigmoid activation function.

|  |  |
| --- | --- |
| Value | Hyperparameter |
| Filters | 32 |
| Kernel Size | 3 |
| Activation | ReLU, Sigmoid |
| Dense Layer | 64 |
| Dropout Rate | 0.2 |
| Loss | Binary Crossentropy |
| Optimizer | Adam |

# Results and Discussions

To detect fraudulent transactions, this study employed a novel hybrid deep learning model that integrated CNN, Autoencoder, and LSTM. Twenty percent of the large dataset was utilized for validation, while the remaining eighty percent was used for training. The autoencoder was trained to extract features and reduce the dimensionality of the data, while the hybrid model was trained for classification. The models demonstrated a rapid training and validation loss decline, stabilizing at values near zero after 10 training epochs, indicating effective learning and minimal overfitting.

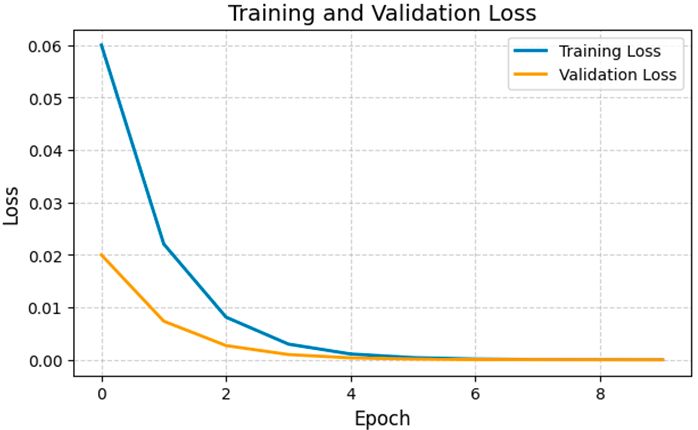


Figure 2. Loss of Training and Validation for Hybrid Model

Effective learning and little overfitting are indicated by the training and validation loss gradually declining, as seen in Figure 2. The accuracy graph illustrates the model's remarkable ability to distinguish between fraudulent and legitimate transactions, showing that it rapidly converged to near-perfect accuracy within a few epochs.

A graph of a training and validation accuracy

AI-generated content may be incorrect.

Figure 3. Accuracy of Training and Validation for Hybrid Model

Both training and validation accuracy rose quickly and converged to almost flawless values in the first epochs, as shown in Figure 3. This shows that the model successfully picked up on the patterns in the dataset, detecting fraudulent transactions with high accuracy and retaining generalization to new data.

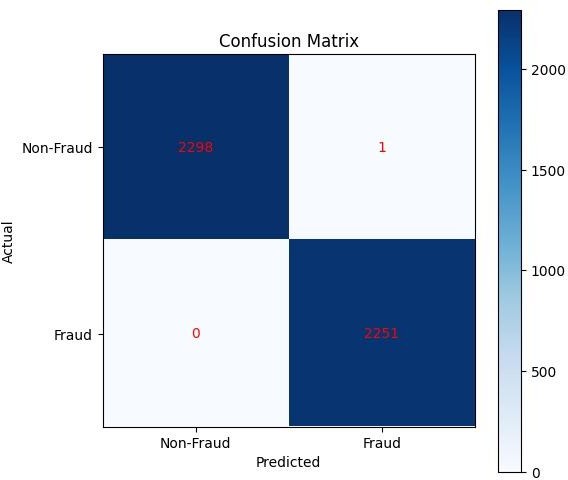


Figure 4. Confusion Matrix for Hybrid Model

With an AUC of 1.00 and 100% test accuracy, our suggested hybrid model showed outstanding performance in identifying credit card fraud, showing faultless categorization. With just one misclassification, the algorithm correctly identified 2,298 fraudulent transactions and 2,252 non-fraudulent transactions. The model's near-perfect detection capacity is demonstrated by the confusion matrix (Figure 4), which emphasizes how well it detects fraudulent transactions while reducing false positives and negatives.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Class** | **Precisio n** | **Reca ll** | **F1-**  **Score** | **Suppo rt** |
| **0.0 (Non-Fraud)** | 1 | 1 | 1 | 2299 |
| **1.0 (Fraud)** | 1 | 1 | 1 | 2251 |
| **Accuracy** |  |  | 1 | 4550 |
| **Macro Avg** | 1 | 1 | 1 | 4550 |
| **Weighted Avg** | 1 | 1 | 1 | 4550 |

Table 1. Summary of Evaluation Metrics for Hybrid Model

The performance characteristics of the proposed model for detecting credit card fraud are shown in Table 1. The model's precision, recall, and F1-score all hit 1.00 for both fraudulent and non-fraudulent transactions, yielding a 100% accuracy rate. The model's resilience in handling both classes is further demonstrated by the weighted

average and macro average scores. These results show the model's ability to accurately classify fraud instances without misclassifications, indicating its high degree of reliability for real-world fraud detection applications.

## Conclusion

Detecting credit card theft is crucial due to the rise in digital transactions. Traditional methods struggle to address class differences and evolving fraud tactics. This paper proposes a hybrid deep learning model that includes SMOTE, Autoencoders, Conv1D, and LSTM to increase accuracy. Local features are recorded by Conv1D, patterns are found by Autoencoders, data is balanced by SMOTE, and temporal correlations are found using LSTM. Experiments on the Credit Card Dataset show better precision, recall, and fraud detection accuracy than traditional models, which reduces false positives. In the future, research will focus on real-time deployment and model interpretability (e.g., SHAP) to increase transparency and flexibility in fraud detection.

# References

* 1. Prabha, D. P.; Priscilla, C. V. A Combined Framework Based on LSTM Autoencoder and XGBoost with Adaptive Threshold Classification for Credit Card Fraud Detection. *The Scientific Temper*,2024,*15*(2),2216–2224. DOI:10.58414/SCIENTIFICTEMPER.2024.15.2.34.
  2. Ileberi, E.; Sun, Y. A Hybrid Deep Learning Ensemble Model for Credit Card Fraud Detection. IEEEAccess,2024, DOI:10.1109/ACCESS.2024.3502542.
  3. Sulaiman, S. S.; Nadher, I.; Hameed, S. M. Credit Card Fraud Detection Using Improved Deep Learning Models. *Computer Science Journal*, 2024, *Vol. 18*, 1001–1015.
  4. I. D. Mienye and N. Jere, "Deep Learning for Credit Card Fraud Detection: A Review of Algorithms, Challenges, and Solutions," *IEEE Access*, vol.12, pp. 96893–96912,Jul.2024,

doi: 10.1109/ACCESS.2024.3426955.

* 1. F. K. Alarfaj and S. Shahzadi, "Enhancing Fraud Detection in Banking with Deep Learning: Graph Neural Networks and Autoencoders for Real-Time Credit Card Fraud Prevention," *IEEE Access*, vol. 13, pp.20633-206502025, doi: 10.1109/ACCESS.2025.XXXXXXX.
  2. Iseal, S.; Ibrahim, J.; Wasiu, S.; Daniel, **S.** Improving Financial Fraud Detection with Deep Learning Algorithms. *In Proceedings of the International Economics and Economic Policy,* Volume 9, Issue 11, November 2024; Western University: Ontario, Canada, 2024; pp. a479– c486.
  3. Dhandore, D.; Agrawal, C.; Meena, P. Enhancing Credit Card Fraud Detection through Advanced Ensemble Learning Techniques and Deep Learning Integration. *In Proceedings of the International Journal of Engineering Applied Science and Management,* Volume 5, Issue 9, September 2024; Radharaman Institute of Technology and Science: Bhopal, India, 2024; pp. a479–c486.
  4. Palivela, H.; Rishiwal, V.; Bhushan, S.; Alotaibi, A.; Agarwal, U.; Kumar, P.; Yadav, M. Optimization of Deep Learning-Based Model for Identification of Credit Card Frauds. *In Proceedings of the IEEE Access,* Vol. 12, 2024; IEEE: Dubai, United Arab Emirates,2024; pp.125629–125636. <https://doi.org/10.1109/ACCESS.2024.3440637>
  5. San Miguel Carrasco, R.; Sicilia-Urbán, M.-Á. Evaluation of Deep Neural Networks for Reduction of Credit Card Fraud Alerts. *In Proceedings of the IEEE Transactions on Neural Networks and Learning Systems,* Vol. 8, 2020; IEEE: Madrid, Spain, 2020; pp. 186421–186432. <https://doi.org/10.1109/TNNLS.2020.2995231>
  6. 1. Shankar RS, Mahesh G, Maheswararao V, Silpa N, Murthy KV. Mitigating Misinformation: An Advanced Analytics Framework for Proactive Detection of Fake News to Minimize Misrepresentation Risks. Algorithms in Advanced Artificial Intelligence: ICAAAI-2023. 2024 Jul 8:289.
  7. 2. Pradhan SN, Shankar RS, Barik S, Mohanty B, Rao VR. Evaluation of stress based on multiple distinct modalities using machine learning techniques. International Journal of Public Health. 2024 Jun;13(2):944-54.
  8. 3. Venkata VM, Gupta KR, Krishna CV, Murthy KV, Shankar RS. Validation on selected breast cancer drugs of physicochemical features by using machine learning models. International Journal of Public Health. 2024 Jun;13(2):794-803.
  9. 4. Reddy SS, Gupta VM, Srinivas LV, Swaroop CR. Methodology for eliminating plain regions from captured images. Int J Artif Intell ISSN.;2252(8938):1359.
  10. 5. Mahesh G, Shankar RS, Rao VM, Silpa N. An Object Detection Framework and Deep Learning Models Used to Detect the Potholes on the Streets. In2024 International Conference on Advances in Modern Age Technologies for Health and Engineering Science (AMATHE) 2024 May 16 (pp. 1-7). IEEE.
  11. 6. Murthy KV, Rajanikanth J, Shankar RS, Swaroop CR, Ravibabu D. Generative AI in Personal Dairy Information Retrieval for Criminal Investigation. In Algorithms in Advanced Artificial Intelligence 2024 (pp. 507-513). CRC Press.
  12. 7. Gupta VM, Shankar RS, Murthy KV, Mahalakshmi CH. An approach for prediction of weather by using feed-forward neural networks. In AIP Conference Proceedings 2023 Dec 15 (Vol. 2901, No. 1). AIP Publishing.
  13. 8. Mahesh G, Varma KV, Shankar RS, Murthy KR. Multiclass Prediction of Pneumonia based on X-rays by using Mining Techniques. In2023 Third International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS) 2023 Sep 1 (pp. 188-194). IEEE.
  14. 9. Shiva Shankar R, Neelima P, Priyadarshini V, Murthy KV. Comprehensive Analysis to Predict Hepatic Disease by Using Machine Learning Models. In Mobile Computing and Sustainable Informatics: Proceedings of ICMCSI 2022 2022 Jul 16 (pp. 475-490). Singapore: Springer Nature Singapore.
  15. 10. Punuri SB, Kuanar SK, Mishra TK, Rao VV, Reddy SS. Decoding Human Facial Emotions: A Ranking Approach using Explainable AI. IEEE Access. 2024 Oct 4..